Služby přenosu souborů

http://www.explorer.cz/cz/publish/43/Ftp-prenos-souboru.html
http://4iz110.vse.cz:41004/4iz110/cv4/cv4.html

FTP

- protokol, ale i název služby
- určen pro předávání souborů ze serveru a na server
- pracuje na **aplikační vrstvě**
- jedná se o jeden z nejstarších protokolů a zároveň nejčastěji používanou službu pro předávání dat na Internetu
- funguje na principu **klient - server**
- používá **interaktivní** styl komunikace, umožňuje řízení přístupu (přihlašování login/heslo)
- **porty**
  - **TCP/21** - slouží k řízení, jsou jím přenášeny příkazy
  - **TCP/20** - slouží k vlastnímu přenostu dat

Přenos dat

- přenos dat je **8-bitový**
- **2 režimy** přenosu dat
  - **textový** - dochází ke **konverzi konců řádků**, pokud je zdrojový a cílový systém rozdílný - DOS/Windows používá jako konce řádků posloupnost znaků `CR LF`, unixové systémy (Linux, nové verze MacOS) používají pouze znak `LF`
  - **binární** - v binárním režimu není do dat nijak zasahováno (typicky obrázky, komprimované soubory (RAR, ZIP, ...), atp.)

Nejčastější použití

- **sdílení dat** (hudba, videa, vlastní tvorba, apod.) - *v tomto ohledu ztrácí FTP svou dřívější pozici, protože většina uživatelů (především méně technicky zdatných) používá na použití jednodušší a přístupnější sdílecí servery (ulož.to, czshare.com, ...)*
- **správa** účtů internetových **stránek** (nahrávání zdrojových souborů na server - PHP skriptů, HTML stránek, obrázků,...)

Jak protokol funguje

- FTP server poskytuje data pro ostatní počítače. Klient se k serveru připojí a může provádět různé operace (výpis adresáře, změna adresáře, přenos dat atd.). Operace jsou řízeny sadou příkazů, které jsou definovány v rámci FTP protokolu, proto kdokoliv může vytvořit klienta pro jakékoliv prostředí nebo operační systém.

- Stanoví se pravidla komunikace mezi klientem a serverem. Jedná se o spojovanou spolupráci. Klient naváže spojení se serverem, předá uživatelské jméno a heslo. Po navázání spojení může probíhat práce s adresáři a soubory a přenos dat mezi klientem a serverem. Spojení se obvykle ukončí z podnětu klienta. Úsek

komunikace mezi otevřením a uzavřením spojení se nazývá *relace*.
- V případě protokolu FTP se užívá na straně serveru dvou standardních portů (20 a 21). Server na nich očekává a vyřizuje požadavky klientů. Pakety na portu 21 slouží k řízení komunikace - *řídicí kanál*. Port 20 slouží k vlastnímu přenosu dat - *datový kanál*. Porty na straně klienta jsou dynamicky přidělované a přiděluje je OS.
- Řídicí kanál se po dobu relace otevře jen jednou a zůstává otevřen, zatímco datový se po přenosu dat (souboru) uzavře a pro každý datový přenos je nutné kanál znovu otevřít.
- Podle toho, kdo otevírá datový kanál, se rozlišuje aktivní a pasivní režim spojení. Přenos souborů probíhá v textovém nebo binárním režimu v závislosti na typu souboru nebo potřebách uživatele. Chování serveru nebo klientského programu je určeno konfigurací. O komunikaci lze vést na obou stranách spojení protokol.

Anonymní a neanonymní služba přenosu souborů

- **Anonymní servery** umožňují přihlášení uživatele pomocí předem daného a pro všechny uživatele společného uživatelského jména - např. `anonymous` nebo `ftp`. K zadání hesla obvykle stačí adresa elektronické pošty. Tyto servery umožňují prohlížení veřejně přístupných adresářů a stahování souborů na lokální počítač. Zpravidla nepovolují zápis do struktury souborů serveru.

- **Neanonymní servery** vyžadují účet uživatele pro daný server. Účet se skládá se z přihlašovacího jména a hesla. Server určuje oprávnění uživatele k souborům a adresářům. Seznam účtů vytváří správce služby.

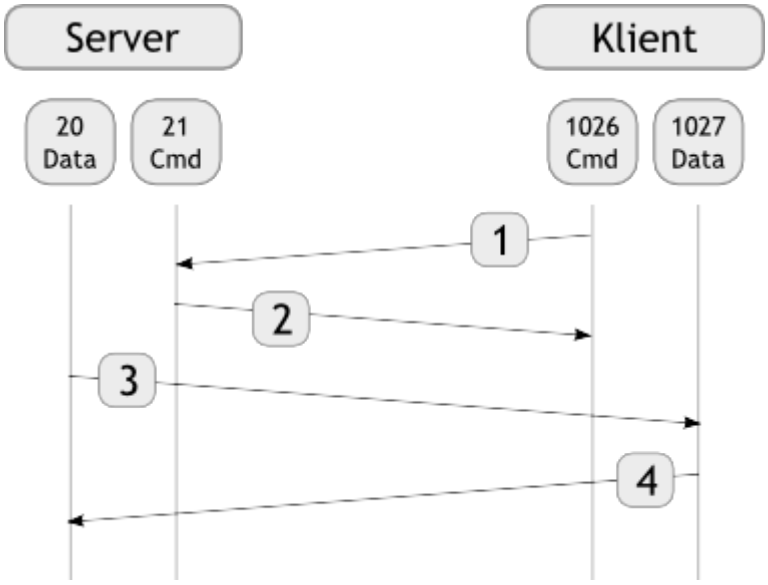
Aktivní a pasivní režim spojení

- připojení k FTP serveru je možné realizovat v aktivním nebo pasivním režimu. Pasivní režim je bezpečnější, ale ne vždy je technicky realizovatelný
- druh spojení je určen podle toho, kdo otevírá datový kanál (klient / server)

Aktivní režim

- jestliže datový kanál **otevírá server**, jde o aktivní režim spojení
- na portu **TCP/20** jsou přenášena data (*data connection*)
- připojení na přenos dat navazuje server a **klient naslouchá**
- klient oznámí serveru příkazem `PORT` svou IP adresu a port, kde bude očekávat příchod datových paketů serveru
- **problém** zpravidla nastává, když se klient připojuje z privátní sítě a jeho adresa je překládána pomocí NATu

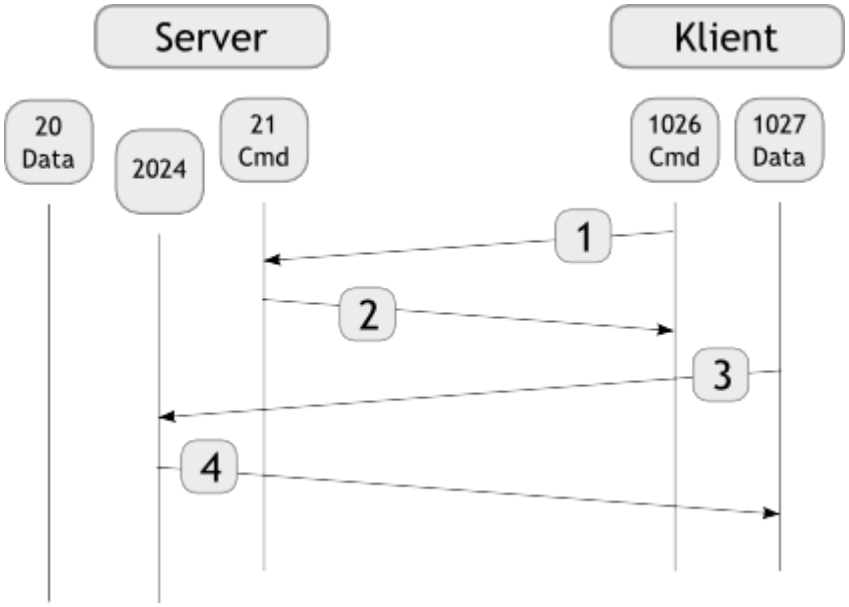
```
PORT 146,102,64,219,4,150
200 command successfully executed
```



Pasivní režim

- připojení pro přenos dat (*data connection*) **navazuje klient**, server naslouchá
- při sestavování *data connection* pošle server klientovi svou IP adresu a TCP port, na kterém server naslouchá a čeká na přenesení dat
- klient nejdříve požádá server příkazem `PASV`, aby přešel do pasivního režimu
  - pokud server souhlasí, pošle na řídícím kanálu odpověď s uvedením své IP adresy a portu, na němž datové spojení očekává

```
PASV
227 Entering Passive Mode (195,113,144,229,220,154)
```



Programy

Serverové programy

- existuje velké množství programů, které fungují jako **FTP server**
- např. **VSFTP**, **ProFTP** a mnoho dalších

Klientské programy

- pro práci s FTP existuje **velké množství** programů - jak **textových** (pro příkazový řádek), tak i **grafických**
- **textově orientované** - např. `lftp`, **MS FTP** - výchozí textový klient ve Windows (příkaz `ftp`) a řada dalších
- **graficky orientované** - v současné době nad textovými klienty převládají
  - čistokrevní FTP klienti - např. **FileZilla**, gFTP (na Linuxu), apod.
  - FTP klienti jako součást správce souborů - např. **Total Commander**, **Průzkumník** ve Windows (program `explorer.exe`), ...
  - FTP integrované do webového prohlížeče - Opera, Firefox, ... - většinou umožňují pouze čtení souborů z FTP serveru - ale už nikoli vytvářet, mazat, nahrávat a editovat soubory a adresáře

Výhody

- serverová část je jednodušší, než běžný HTTP server (neplatí pro odlehčené HTTP servery)
- na rozdíl od HTTP má protokol širší možnosti (nastavení práv, mazání, upload, ...)

Nevýhody

- hesla a soubory jsou ve standardním protokolu zasílána jako běžný text (nejsou šifrovaná)
  - snižuje bezpečnost (ohrožuje jméno, heslo, ale i přenášená data)
  - existují rozšíření FTP protokolu, která tento nedostatek odstraňují (např. FTPS)
- FTP server má delší odezvy
  - nemožnost sloučit přenos více (malých) souborů do jednoho zvyšuje časovou režii i zátěž serveru
- v některých sítích je povolen pouze protokol HTTP (tj. povoleno pouze prohlížení webových stránek) - v takových sítích není možné protokol FTP použít

Zabezpečení

- FTP protokol v současné době už **není** považován za **bezpečný** ☐ byla pro něj definována některá rozšíření
- možnosti zabezpečení komunikace:
  1. **VPN** - privátní tunel, jedná se o zabezpečenou komunikaci i když FTP zabezpečeno není (šifrován je vlastní tunel, nikoli samotná FTP komunikace)
  2. **FTPS** - obdoba HTTPS (předají si klíče, pak šifrují)
  3. **SFTP**- postaveno nad jiným zabezpečeným protokolem (nejčastěji SSH)
  4. **SCP** - oproti SFTP má omezené možnosti (není tak komplexní)
     - programy - např. WinSCP, Putty (terminál),...

FTPS (FTP s podporou SSL/TLS)

- klient se připojuje na port 21, zahajuje nešifrovanou komunikaci a žádá o aktivaci TLS (SSL) před tím, než

budou poslána citlivá data
- protokol TLS umožňuje aplikacím komunikovat po síti způsobem, který zabraňuje odposlouchávání či falšování zpráv
- pomocí kryptografie poskytuje TLS svým koncovým bodům autentizaci a soukromí při komunikaci Internetem
- typicky je autentizován pouze server (tedy jeho totožnost je zaručena), zatímco klient zůstává neautentizován
- to znamená, že koncový uživatel (ať člověk či aplikace - např. webový prohlížeč) si může být jist s kým komunikuje
- Další úroveň zabezpečení, při níž oba konce „konverzace“ mají jistotu s kým komunikují, je označována jako vzájemná autentizace
- Vzájemná autentizace vyžaduje nasazení infrastruktury veřejných klíčů (PKI) pro klienty

- TLS zahrnuje **3 základní fáze**
  - dohodu účastníků na podporovaných algoritmech
  - výměnu klíčů založenou na šifrování s veřejným klíčem a autentizaci vycházející z certifikátů
  - šifrování provozu symetrickou šifrou

SFTP (Secure FTP) a SCP (Secure Copy)

- **SFTP**
  - pro přenos dat obvykle využívá protokol **SSH-2**
  - je ale navržen tak, aby ho bylo možné používat i nad jiným protokolem
  - narozdíl od SCP má široké možnosti pro doplňující operace se soubory - umožňuje pokračovat v přerušených přenosech, vypisovat adresáře i odstraňovat soubory na vzdáleném počítači

- **SCP**
  - jednoduchý protokol
  - pro šifrování a autentizaci využívá protokol SSH

- v praxi je rozšířena aplikace **WinSCP** - jedná se o souborový manažer, který je založený na knihovnách Putty (SSH klient) a umožňuje práci v režimu SFTP a SCP.

Pozor! Následující část nesouvisí s protokolem FTP.

SSH

- SSH (Secure Shell) je zabezpečený komunikační protokol
- používají TCP/IP (port 22)
- byl navržen jako náhrada za telnet a další nezabezpečené vzdálené shelly (rlogin, rsh apod.), které posílají heslo v nezabezpečené formě a umožňují tak jeho odposlechnutí při přenosu pomocí počítačové sítě
- šifrování přenášených dat, které SSH poskytuje, slouží k zabezpečení dat při přenosu přes nedůvěryhodnou síť.
- SSH umožňuje bezpečnou komunikaci mezi dvěma počítači, která se využívá

pro zprostředkování přístupu k příkazovému řádku, kopírování souborů, ale také k jakémukoliv obecnému přenosu dat

- také zabezpečuje autentizaci obou účastníků komunikace, transparentní šifrování

přenášených dat, zajištění jejich integrity a volitelnou bezeztrátovou kompresi

- **Výhody**
  - narozdíl od svých předchůdců používá SSH zabezpečený (šifrovaný) komunikační kanál